1. A computer server system for managing digital identity information, comprising at least one processor in operable connection with a memory configured by a database, the database including at least one user object for a user, the user object having a corresponding safe object in the database for the user, the safe object containing at least one profile administered by the user, each profile including digital identity information provided by the user.

2. The system of claim 1, wherein at least one safe object contains more than one user-administered profile and different profiles provide sets of different digital identity information about the user.

3. The system of claim 1, wherein the safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe which receives controlled read access to digital identity information from at least one of the profiles.

4. The system of claim 1, wherein the safe object also contains at least one drop box object.

5. The system of claim 1, wherein the safe object also contains at least one application object with settings for an application.

6. The system of claim 1, wherein the safe object also contains at least one view object.

7. The system of claim 1, wherein the safe object also contains at least one access object.

8. The system of claim 1, wherein the system comprises a web server and an identity server.

9. The system of claim 8, wherein the web server and the identity server communicate using encrypted usernames.

10. The system of claim 8, wherein the web server and the identity server are secured by a firewall.

11. The system of claim 1, wherein the system comprises an identity server appliance.

12. The system of claim 1, further comprising a zero-byte client.

13. The system of claim 1, further comprising an installed client.

14. The system of claim 1, wherein the system comprises a provider model for access to the database, and the provider model abstracts the details of a particular directory and storage protocol.

15. The system of claim 1, wherein the system comprises an abstract model for access to the database, and the abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data.

16. The system of claim 1, wherein the system comprises a programmatic interface to identity items and operations that correspond generally to directory service objects.

17. The system of claim 1, wherein the database includes multiple safe objects contained in a vault object.

18. The system of claim 17, wherein the system includes at least two vault objects hosted on different servers, each vault object contains at least one user safe

object, and objects contained by the safe objects are federated to provide controlled access between the vault servers.

19. The system of claim 18, wherein the objects are federated using a Universal Resource Identifier which specifies at least a protocol, a host, a path, and an object.

20. The system of claim 1, further comprising a digital business card application object having a corresponding profile object which includes digital identity information provided by the user.

21. The system of claim 1, wherein the system comprises a means for one user to receive updated profile information of another user using a link to the database.

22. The system of claim 1, wherein the database is a partitioned directory services database.

23. The system of claim 1, wherein the system is further characterized in that it provides an account creation service which creates a new account for a user based on a template.

24. The system of claim 1, wherein the system is further characterized in that it provides a safe management service which provides an administrative tool to manage and maintain safe objects.

25. The system of claim 1, wherein the system is further characterized in that it provides a schema management service which permits an administrator to at least view a directory service schema.

26. The system of claim 1, wherein the system is further characterized in that it provides a batch account creation service which creates several accounts at one time.

27. The system of claim 1, wherein the system is further characterized in that it provides an install service which permits one to install and configure an identity server.

28. The system of claim 1, wherein the system is further characterized in that it provides a backup and restore service which allows one to backup and restore at least one safe object.

29. The system of claim 1, wherein the system is further characterized in that it provides a safe advisor service which allows one to verify the integrity of a safe object.

30. The system of claim 1, wherein the system is further characterized in that it provides a legal recovery tool which recovers digital identity information for forensic use.

31. The system of claim 1, wherein the system is further characterized in that it provides a data denormalization service which facilitates data transformation on database fields.

32. The system of claim 1, wherein the system is further characterized in that it provides a rules service.

33. The system of claim 1, wherein the system is further characterized in that it provides an event service which allows an identity server to register interest in and be notified of changes in the database.

34. The system of claim 1, wherein the system is further characterized in that it provides an identity verification service which allows one to verify the identity of a user based on registration information.

35. The system of claim 1, wherein the system is further characterized in that it provides an authorization service which allows a process to verify information gathered from a user registration form.

36. The system of claim 1, wherein the system is further characterized in that it provides a profile discovery and publishing service which allows users to publish at least a portion of their profile information.

37. The system of claim 1, wherein the system is further characterized in that it provides a form fill-in service which allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects.

38. The system of claim 1, wherein the system is further characterized in that it provides a form conversion service which assists a webmaster in converting existing forms to standardized field names.

39. The system of claim 1, wherein the system is further characterized in that it provides an install service which installs servlets on a web server.

40. The system of claim 1, wherein the system is further characterized in that it provides an identity exchange service for portions of a privacy protection protocol.

41. The system of claim 1, wherein the system is further characterized in that it provides a chat service which sets up chat rooms so users can communicate with each other in real time.

42. The system of claim 1, wherein the system is further characterized in that it provides a presence service which lets users specify where they are and allows them to discover another user's presence information.

43. The system of claim 1, wherein the system is further characterized in that it provides an anonymous remailer service which allows users to choose different email addresses for different profiles.

44. The system of claim 1, wherein the system is further characterized in that it provides an anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information.

45. The system of claim 1, wherein the system is further characterized in that it provides an infomediary service which facilitates creating an infomediary.

46. The system of claim 1, wherein the system is further characterized in that it uses profile objects and software for tracking IP addresses in order to selectively publish the last known IP address of a user.

47. The system of claim 1, wherein the system is further characterized in that it uses profile objects and at least one of an underlying directory service and an underlying file system in order to enforce access controls on web pages published by users.

48. The system of claim 1, wherein the system is further characterized in that it provides email services.

49. The system of claim 48, wherein the user has an email address, and the system encodes contact relationship information in the user's email address.

50. The system of claim 48, wherein the system uses profiles to filter email sent to the user.

51. The system of claim 1, further comprising a means for determining whether a user logging in at a third party web site is registered as a user of the system.

52. The system of claim 51, further comprising a means for logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered.

53. The system of claim 52, wherein the means for registering the user and logging the user in comprises a means for capturing user login information for the third party web site.

54. The system of claim 1, wherein the system is further characterized in that user digital identity information is only made available to a partner site if the user has flagged the information as public.

55. The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a transaction history.

56. The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a user authentication mechanism.

57. The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a launch point for launching application programs.

58. The system of claim 1, wherein the system is further characterized in that it uses a non-repudiation feature whereby an administrator cannot change a user password and then log on as the user.

59. A computer client system for managing digital identity information, comprising a processor in operable connection with a memory configured for communication with at least one server computer using a browser, the system further characterized in that it provides a user interface for user administration of a database

which includes multiple profiles of the user that are administered by the user, each profile including digital identity information provided by the user.

60. The system of claim 59, wherein the client system comprises a zero-byte client.

61. The system of claim 59, wherein the client system comprises an installed client.

62. The system of claim 59, wherein the client system comprises an application program.

63. The system of claim 59, wherein the system comprises a provider model for access to the database, and the provider model abstracts the details of a particular directory and storage protocol.

64. The system of claim 59, wherein the system comprises an abstract model for access to the database, and the abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data.

65. The system of claim 59, wherein the system comprises a programmatic interface to identity items and operations that correspond generally to directory service objects.

66. The system of claim 59, wherein the user interface comprises a screen for creating a user contact.

67. The system of claim 59, wherein the user interface comprises a screen for sharing a user contact.

68. The system of claim 59, wherein the user interface comprises a means for indicating that access to the user's identity information has been revoked by the user.

69. The system of claim 59, wherein the system further comprises software for tracking IP addresses in order to facilitate selectively publishing the last known IP address of the user.

70. The system of claim 59, wherein the user interface allows the user to specify access controls on web pages published by the user.

71. The system of claim 59, wherein the user interface allows the user to specify email blocking using a profile of the user.

72. The system of claim 59, wherein the system is further characterized in that it uses an embossed icon which provides a transaction history.

73. A method for managing digital identity information, comprising the computer-assisted steps of:

obtaining from a user first digital identity information of the user;

causing the first digital identity information to be placed in a first profile in a database;

obtaining from the user second digital identity information of the user;

causing the second digital identity information to be placed in a second profile in the database;

providing the user with access to the profiles to allow the user to update the digital identity information while denying such access to other entities; and

providing an entity other than the user with read-only access to a profile of the user in response to instructions from the user.

74. The method of claim 73, wherein the method further comprises creating a contact list for the user in response to instructions from the user.

75. The method of claim 73, wherein the method further comprises automatically logging the user into a web site using at least part of the digital identity information from a profile of the user.

76. The method of claim 73, wherein the method further comprises automatically filling in a web form using at least part of the digital identity information from a profile of the user.

77. The method of claim 73, wherein the method further comprises capturing login information of the user for a web site and storing at least part of the captured information in the database.

78. The method of claim 73, wherein the step of providing an entity other than the user with read-only access comprises beaming the profile over a wireless link.

79. The method of claim 73, wherein the method further comprises revoking access to a profile of the user and subsequently denying read-only access which was previously allowed.

80. The method of claim 73, wherein the method further comprises restricting access to web pages of the user based at least in part on a profile of the user.

81. The method of claim 73, wherein the method further comprises encoding contact relationship information in an email address of the user.

82. The method of claim 73, wherein the method further comprises using a profile to filter email sent to the user.

83. A configured computer-readable storage medium for managing digital identity information, the storage medium configured to perform the steps of:

obtaining from a user first digital identity information of the user;

causing the first digital identity information to be placed in a first profile in a database;

obtaining from the user second digital identity information of the user;

causing the second digital identity information to be placed in a second profile in the database;

providing the user with access to the profiles to allow the user to update the digital identity information while denying such access to other entities; and

providing an entity other than the user with read-only access to a profile of the user in response to instructions from the user.

84. The configured storage medium of claim 83, wherein the method further comprises creating a contact list for the user in response to instructions from the user.

85. The configured storage medium of claim 83, wherein the method further comprises automatically logging the user into a web site using at least part of the digital identity information from a profile of the user.

86. The configured storage medium of claim 83, wherein the method further comprises automatically filling in a web form using at least part of the digital identity information from a profile of the user.

87. The configured storage medium of claim 83, wherein the method further comprises restricting access to web pages of the user based at least in part on a profile of the user.

88. The configured storage medium of claim 83, wherein the method further comprises encoding contact relationship information in an email address of the user.

89. The configured storage medium of claim 83, wherein the method further comprises using a profile to filter email sent to the user.